TELKOMNIKA, Vol.12, No.1, March 2014, pp. 23~32
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v12i1.1272

The Analysis and Application on a Fractional-Order Chaotic System

Lihua Zhou*[1], Ye Qian[2], Lingliang Liu[3]
[1] Department of Computer Science and Engineering, School of Information, Yunnan University, Kunming 650091, P.R. China
[2] School of Software Yunnan University, Kunming 650091, China
[3] Agricultural Bank of China Branches in Hubei province, Wuhan 430071, China
*Corresponding author, e-mail: lhzhou@ynu.edu.cn

Abstract

An integral-order hyperchaotic system with four-dimension is expanded to be a fractional-order system whose chaotic behaviors are analyzed, Firstly, based on the stability theory of fractional-order linear system and the thinking of tracking control, a synchronization method for two fractional-order systems with different structures is proposed, and an analytic expression for synchronization controller is given. Secondly, taking the extended fractional-order system and Rőssler hyperchaotic system as example, the synchronization between them is numerical simulated. Finally, the proposed synchronization method is applied to encrypt and decrypt digital images. The simulation results show that the lowest order that extended fractional-order system appears chaos is 3.2, and this method has many advantages for encrypting and decrypting digital images, such as sensitive secret keys, random uniform distribution of pixels and low correlation between adjacent pixels.

Keywords: *Chaos; fractional-order chaotic system; chaotic synchronization; image encryption*

1. Introduction

Chaos is a random, uncertain and never repeated movement happened in particular systems and it expresses the properties of a system, such as complexity, disorder and randomness [1]. Because chaos is a universal phenomenon in the natural world, it is helpful to make research on chaos for promoting the development of many disciplines. Meanwhile, the development of these disciplines can also expand application fields of chaos. At present, the research on the control of chaos synchronization, hyperchaos, chaotic neural networks, chaotic secure communication, and chaotic economics etc. shows potential value of chaos.

In recent years, some unique properties that only exist in fractional-order rather than integer-order dynamics system have been found via incorporating fractional-order differential operator with any real constants into nonlinear dynamic system. For example, an integer-order nonlinear system whose order is less than three does not induce any chaotic phenomenon, but it appears in Chuas circuits with 2.7 orders [2], it also appears in the heteronomy Duffing system whose order is less than two [3] and Rossler equation with 2.4 order [4]. It has been found that a chaotic system still presents chaotic state after fractional-order differential operator is incorporated into it. Furthermore, a fractional-order chaotic system has more complex dynamic characteristics and shows more physical phenomena than integer-order chaotic system. The research on fractional-order chaotic systems has received a great deal of attention.

There are two problems in the research on the fractional-order chaotic systems are quite deserving our attention. One is that on what condition a fractional-order system is in chaotic state when its corresponding ordinary differential system is in chaotic state, and the other is how to design the controller to synchronize two fractional-order chaos systems with different structures. Because fractional-order chaotic systems are different from integer-order chaotic systems in characteristics, the classical controller and synchronization methods for integer-order chaotic systems can not be extended to fractional-order chaotic systems, and a novel approach is indispensable.

In this paper, a four-dimensional integral-order hyperchaotic system proposed in [5] is expanded to be a fractional-order system. Firstly, some chaos characteristics of the fractional-order system are theoretically analyzed and quantitatively simulated. Secondly, based on the stability theory of fractional-order linear system and the thinking of tracking control [6], a method

Received March 24, 2013; Revised October 13, 2013; Accepted October 28, 2013

to synchronize two fractional-order chaos systems with different structures is put forward. Thirdly, the analysis formula of synchronous controller is given, and the synchronization between the extended fractional-order system and Rőssler hyperchaotic system is quantitatively simulated. Finally the proposed synchronization method is applied to encrypt and decrypt digital images. The results show that this method has many advantages for encrypting and decrypting digital images.

2. Related Work

The mathematical model of the four-dimensional integral-order hyperchaotic system proposed in [5] is as follows formula (1).

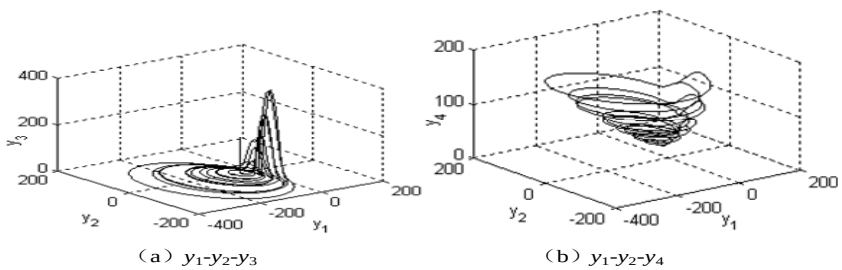
$$\begin{cases} \dfrac{dx_1}{dt} = \dot{x}_1 = a(x_2 - x_1), \\ \dfrac{dx_2}{dt} = \dot{x}_2 = bx_1 + x_1x_3 - x_4, \\ \dfrac{dx_3}{dt} = \dot{x}_3 = -x_1x_2 - cx_3 + x_4, \\ \dfrac{dx_4}{dt} = \dot{x}_4 = dx_1 + x_2. \end{cases} \tag{1}$$

$$\begin{cases} \dfrac{d^{\alpha} y_1}{dt^{\alpha}} = -(y_2 + y_3), \\ \dfrac{d^{\alpha} y_2}{dt^{\alpha}} = y_1 + \tilde{a} y_2 + y_4, \\ \dfrac{d^{\alpha} y_3}{dt^{\alpha}} = \tilde{b} + y_1 y_3, \\ \dfrac{d^{\alpha} y_4}{dt^{\alpha}} = -\tilde{c} y_3 + \tilde{d} y_4. \end{cases} \tag{2}$$

Where x_1, x_2, x_3, x_4 and a, b, c, d are state variables and parameters of system respectively. This system was found to be chaotic in a wide parameter range. In [5], when $a=10$, $b=35$, $c=1.4$, $d=5$, the system (1) is hyperchaotic, and the Lyapunov exponent of system is $\lambda_{L_1} = 0.8058$, $\lambda_{L_2} = 0.0981$, $\lambda_{L_3} = 0$ and $\lambda_{L_4} = -12.3058$.

Rőssler system [7,8], firstly proposed by Rőssler in 1979, is a famous 4-dimensional hyperchaotic system. The system is described in formula (2), where the parameters are $\tilde{a} = 0.32, \tilde{b} = 3, \tilde{c} = 0.5, \tilde{d} = 0.05$.

The phase portrait of fractional-order Rőssler hyperchaotic system is shown in Figure 1. The system (2) has been studied and implemented by many researchers via mathematical theory and electronic oscillators, and it has been extensively applied in various fields, such as secure communications, synchronization, and lasers. So it is chosen to be synchronization with fractional-order chaos systems proposed in this paper.



(a) y_1-y_2-y_3 (b) y_1-y_2-y_4

Figure 1. Phase portrait of fractional-order Rossler hyperchactic system α=0.5

The classical methods for solving fractional-order differential equations include Quadrature Methods, Adams-Bashforth-predictor-corrector method, and the short memory principle method based on Grunwald-Letnikov [9]. Considering time domain methods for simulating fractional-order system are complicated and these methods require very long simulation time, the short memory principle method based on Grunwald-Letnikov [9] is applied in this paper. This method can reduce computation cost than time domain method and get more reliable results than frequency calculation method [10].

Applying chaos to encrypt data was firstly put forward by Matthews [11]. With the development of chaos synchronization, applying chaos synchronization to encrypt digital images has received a great deal of attention [12, 13, 14]. Because fractional-order chaotic systems have more memory function and more easy stability than integer-order system, it can improve control accuracy and has more privacy and robustness to use fractional-order chaotic systems as signal carrier.

3. The Description and Analysis of Fractional-Order Chaotic System

The integral-order differential is replaced with fractional-order differential and the state variable x_3 is added to the first equation in the system (1), by this way, a integral-order system is expanded to be a fractional-order system that is shown in formula (3).

$$\begin{cases} \dfrac{d^{\alpha}x_1}{dt^{\alpha}} = a(x_2 - x_1) + x_3, \\ \dfrac{d^{\alpha}x_2}{dt^{\alpha}} = bx_1 + x_1x_3 - x_4, \\ \dfrac{d^{\alpha}x_3}{dt^{\alpha}} = -x_1x_2 - cx_3 + x_4, \\ \dfrac{d^{\alpha}x_4}{dt^{\alpha}} = dx_1 + x_2. \end{cases} \tag{3}$$

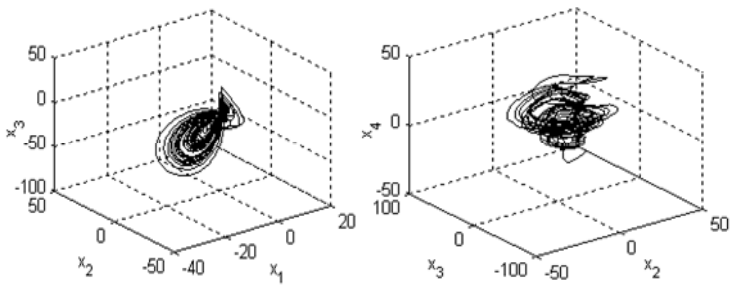
$$\begin{cases} a(x_2 - x_1) + x_3 = 0, \\ bx_1 + x_1x_3 - x_4 = 0, \\ -x_1x_2 - cx_3 + x_4 = 0, \\ dx_1 + x_2 = 0. \end{cases} \tag{4}$$

Where α is the fraction, i.e. $0 < \alpha$ and $n-1 \le \alpha < n$, n is an integer. Let the parameters of system (3) be $a = 8, b = 20, c = 1.1, d = 3$ .In order to find equilibrium points of the system (3), set each equation in (3) equals to zero, which is shown in formula (4).

Two equilibrium points, $O_1(0,0,0,0)$ and $O_2(14.7210,0.4343,-1.029,13.8971)$, can be found by solving equations (4). According to Routh-Hurwitz condition [15], O_1 is an unstable saddle point, because the eigenvalues of Jacobian matrix at O_1, $\lambda_1 = -17.2942$, $\lambda_2 = 9.1148$, $\lambda_3 = 0.0950$ and $\lambda_4 = -1.0155$, are all real, but not all are negative. The eigenvalues of Jacobian matrix at O_2 are $\lambda_1 = -13.7606$, $\lambda_2 = -0.2580$, $\lambda_3 = 2.2013+11.6412j$ and $\lambda_4 = 2.2013-11.6412j$, where λ_1 and λ_2 are negative real, λ_3 and λ_4 are conjugate complex roots with positive real part, and their argument is $|\arg(\lambda_3)| = |\arg(\lambda_4)| = arctg(\dfrac{11.6412}{2.2013}) = \dfrac{0.8810\pi}{2}$. According to the stability theory of fractional-order chaos [16], O_2 is an unstable saddle point when $\alpha > 0.8810$. So when $\alpha > 0.8810$, both O_1 and O_2 are unstable saddle points. By

using Wolf method [17], we can calculate the maximum Lyapunov exponent of this fractional-order system and the result is 0.3059.

Based on the method defined by Grünwald-Letnikov (G-L) for fractional-order differential coefficient numerical value [9], numerical simulation of equations (3) is carried out in Matlab. We set the initial state to $(0.1,0.1,0.1,0.1)$ and $\alpha = 0.95$. The trajectories of system (3) in phase portrait of x_1-x_2-x_3 and x_2-x_3-x_4 are shown in Figure 2(a) and Figure 2(b) respectively, and the Poincare section of system (3) is shown in Figure 3.



（a）x_1-x_2-x_3 （b）x_2-x_3-x_4

Figure 2. the trajectory of system (3), $\alpha = 0.95$

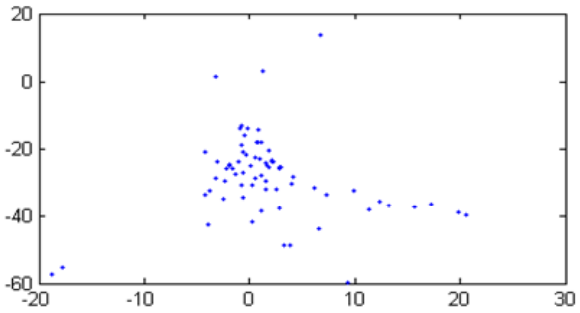


Figure.3 Poincare section of system（3）

In Figure 2(a) and Figure 2(b), the movement in phase space corresponds to random-separation trajectory with no loop. In Figure 3, there are dense points in the Poincare section. Both Figure 2 and Figure 3 illustrate that the system (3) is in chaotic state.

4. The Method to Synchronize Two Fractional-Orders System with Different Structures

In this section, system (3) is appointed as driving system whose state variables are denoted by $\mathbf{x}(t) = (x_1, x_2, x_3, x_4)^T$, Rőssler hyperchaotic system is appointed as responsive system whose state variables are denoted by $\mathbf{y}(t) = (y_1, y_2, y_3, y_4)^T$. A controller is designed to regulate $\mathbf{y}(t)$ to trace $x(t)$.

In order to realize the chaotic synchronization of the two systems, that is, to realize $\lim_{t\to\infty} \|\mathbf{e}(t)\| = \lim_{t\to\infty} \| \mathbf{y}(t) - \mathbf{x}(t) \| = 0$, the fractional-order Rőssler hyperchaotic system is constructed as:

$$\begin{pmatrix} \frac{d^{\alpha} y_1}{dt^{\alpha}} \\ \frac{d^{\alpha} y_2}{dt^{\alpha}} \\ \frac{d^{\alpha} y_3}{dt^{\alpha}} \\ \frac{d^{\alpha} y_4}{dt^{\alpha}} \end{pmatrix} = \begin{pmatrix} -(y_2 + y_3), \\ y_1 + \tilde{a} y_2 + y_4, \\ \tilde{b} + y_1 y_3, \\ -\tilde{c} y_3 + \tilde{d} y_4. \end{pmatrix} + \mathbf{u}(\mathbf{x}(t)) + \mathbf{U}(\mathbf{y}(t), \mathbf{x}(t)) \tag{5}$$

$$\mathbf{f}(\mathbf{x}(t)) = \begin{pmatrix} -(x_2 + x_3) \\ x_1 + \tilde{a} x_2 + x_4 \\ \tilde{b} + x_1 x_3 \\ -\tilde{c} x_3 + \tilde{d} x_4 \end{pmatrix} \tag{6}$$

In formula (5), $\mathbf{u}(\mathbf{x}(t)) + \mathbf{U}(\mathbf{y}(t), \mathbf{x}(t))$ is a tracking controller, in which $\mathbf{u}(\mathbf{x}(t))$ is compensator and $\mathbf{U}(\mathbf{y}(t), \mathbf{x}(t))$ is feedback controller. According to the output of driving system (3), the compensator of responsive system (5) is defined as $\mathbf{u}(\mathbf{x}(t)) = d^{\alpha}\mathbf{x}(t)/dt^{\alpha} - \mathbf{f}(\mathbf{x}(t))$, where formula (6), so controlled fractional-order Rőssler hyperchaotic system (5) can be written as follows:

$$\begin{pmatrix} \frac{d^{\alpha} y_1}{dt^{\alpha}} \\ \frac{d^{\alpha} y_2}{dt^{\alpha}} \\ \frac{d^{\alpha} y_3}{dt^{\alpha}} \\ \frac{d^{\alpha} y_4}{dt^{\alpha}} \end{pmatrix} = \begin{pmatrix} -(y_2 + y_3), \\ y_1 + \tilde{a} y_2 + y_4, \\ \tilde{b} + y_1 y_3, \\ -\tilde{c} y_3 + \tilde{d} y_4. \end{pmatrix} + \begin{pmatrix} \frac{d^{\alpha} x_1}{dt^{\alpha}} \\ \frac{d^{\alpha} x_2}{dt^{\alpha}} \\ \frac{d^{\alpha} x_3}{dt^{\alpha}} \\ \frac{d^{\alpha} x_4}{dt^{\alpha}} \end{pmatrix} - \begin{pmatrix} -(x_2 + x_3) \\ x_1 + \tilde{a} x_2 + x_4 \\ \tilde{b} + x_1 x_3 \\ -\tilde{c} x_3 + \tilde{d} x_4 \end{pmatrix} + \mathbf{U}(\mathbf{y}(t), \mathbf{x}(t)) \tag{7}$$

Let the synchronized error between responsive system and driving system is $e_i = y_i - x_i (i = 1,2,3,4)$, we can obtain the synchronization error system by moving an item in formula (7):

$$\begin{pmatrix} \frac{d^{\alpha} \mathbf{e}_1(t)}{dt^{\alpha}} \\ \frac{d^{\alpha} \mathbf{e}_2(t)}{dt^{\alpha}} \end{pmatrix} = \begin{pmatrix} \mathbf{B}_1 \mathbf{e}_1(t) + \mathbf{F}_1(\mathbf{x}(t), \mathbf{e}_2(t)) \\ \mathbf{B}_2 \mathbf{e}_2(t) + \mathbf{F}_{21}(\mathbf{x}(t), \mathbf{e}_1(t), \mathbf{e}_2(t)) + \mathbf{F}_{22}(\mathbf{x}(t), \mathbf{e}_2(t)) \end{pmatrix} + \mathbf{U}(\mathbf{y}(t), \mathbf{x}(t)) \tag{8}$$

where $\mathbf{F}_1(\mathbf{x}(t), \mathbf{e}_2(t)) = \begin{pmatrix} -e_3 \\ e_4 \end{pmatrix}$, $\mathbf{F}_{21}(\mathbf{x}(t), \mathbf{e}_1(t), \mathbf{e}_2(t)) = \begin{pmatrix} x_3 e_1 + e_1 e_3 \\ 0 \end{pmatrix}$, $\mathbf{F}_{22}(\mathbf{x}(t), \mathbf{e}_2(t)) = \begin{pmatrix} x_1 e_3 \\ 0 \end{pmatrix}$,

$\mathbf{B}_1 = \begin{pmatrix} 0 & -1 \\ 1 & \tilde{a} \end{pmatrix}$, $\mathbf{B}_2 = \begin{pmatrix} 0 & 0 \\ -\tilde{c} & \tilde{d} \end{pmatrix}$, $\mathbf{U}(\mathbf{y}(t), \mathbf{x}(t)) = \begin{pmatrix} \mathbf{A}_1 \mathbf{e}_1(t) - \mathbf{F}_1(\mathbf{x}(t), \mathbf{e}_2(t)) \\ \mathbf{A}_2 \mathbf{e}_2(t) - \mathbf{F}_{22}(\mathbf{x}(t), \mathbf{e}_2(t)) \end{pmatrix}$, the system error $\mathbf{e}(t) = (\mathbf{e}_1(t), \mathbf{e}_2(t))^T$, where $\mathbf{e}_1(t) = (e_1, e_2)^T$, $\mathbf{e}_2(t) = (e_3, e_4)^T$.

We get formula (9) by substituting the feedback controller $\mathbf{U}(\mathbf{y}(t), \mathbf{x}(t))$ in formula (8):

$$\begin{pmatrix} \frac{d^{\alpha}\mathbf{e}_1(t)}{dt^{\alpha}} \\ \frac{d^{\alpha}\mathbf{e}_2(t)}{dt^{\alpha}} \end{pmatrix} = \begin{pmatrix} (\mathbf{B}_1 + \mathbf{A}_1)\mathbf{e}_1(t) \\ (\mathbf{B}_2 + \mathbf{A}_2)\mathbf{e}_2(t) + \mathbf{F}_{21}(\mathbf{x}(t), \mathbf{e}_1(t), \mathbf{e}_2(t)) \end{pmatrix} \quad (9)$$

According to the stability theory of fractional-order linear system [15], if there is a matrix $\mathbf{A}_1 \in R^{2\times 2}$ which in formula (9) meet the need that arguments of all eigenvalues of $\mathbf{B}_1 + \mathbf{A}_1$ are more than $0.5\pi\alpha$, then $\lim_{t\to\infty}\mathbf{e}_1(t) = \lim_{t\to\infty}(y_i - x_i) = 0 \ \ (i = 1,2)$, and when $t \to \infty$, $\lim_{\mathbf{e}_1(t)\to 0}\mathbf{F}_{21}(\mathbf{x}(t), \mathbf{e}_1(t), \mathbf{e}_2(t)) = 0$; if there is a matrix $\mathbf{A}_2 \in R^{2\times 2}$ that meet the need that all eigenvalues of $\mathbf{B}_2 + \mathbf{A}_2$ are more than $0.5\pi\alpha$, then $\lim_{t\to\infty}\mathbf{e}_2(t) = \lim_{t\to\infty}(y_i - x_i) = 0 \ \ (i = 3,4)$. From the above analysis, the aim of $\lim_{t\to\infty}\|\mathbf{e}(t)\| = 0$ can be achieved, so the Rőssler hyperchaotic system can synchronize with driving system (3).

We have implemented synchronization simulation in Matlab. In the experiment, we set $\mathbf{A}_1 = \begin{pmatrix} -5 & 2 \\ -1 & -3.32 \end{pmatrix}, \mathbf{A}_2 = \begin{pmatrix} -3 & 0 \\ 0.5 & -4 \end{pmatrix}$. The eigenvalues of matrix $\mathbf{B}_1 + \mathbf{A}_1, \mathbf{B}_2 + \mathbf{A}_2$ are -5, -3 and -3, -3.95 respectively with the arguments of them satisfying the condition $|\arg\lambda_{\pm}| = \pi > 0.5\pi\alpha$. Initial state of driving system (3) and responsive system (5) are set to $(8,4,2,1)$ and $(-50,-10,160,40)$ respectively, and the synchronous courses of two systems variables are shown in Figure 4, and the synchronization error curve of these two systems is shown in Figure 5. We can see that there is difference between each pair of variables of two systems at the beginning, but they can achieve synchronization step by step by tracking.

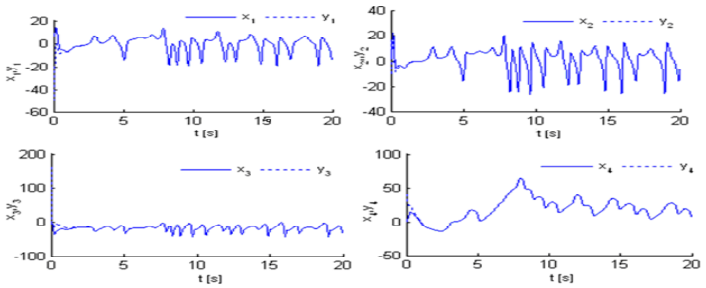


Figure 4. synchronous process of two systems

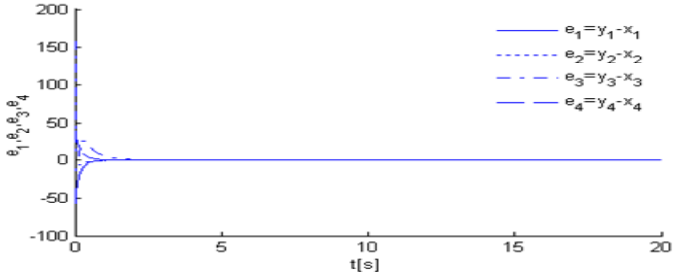


Figure 5. the error curve of these two systems in the synchronization

5. The Application of Chaotic Synchrony in Image Encryption

The process of the applying chaotic synchrony to encrypt and decrypt digital image is shown in Figure 6.

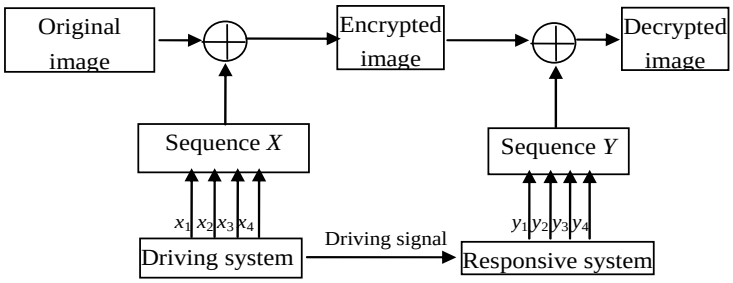


Figure 6. The process of applying chaotic synchrony to encrypt and decrypt Image

The original image is denoted by matrix $G = (g_{ij})_{M \times N}$, where *M* and *N* represent row and column of the image respectively, and g_{ij} is the gray value of the pixel which is at row i and column j of this image, with gray value depth set to *A* (typically *A*=256). The encryption process is completed according to the following steps:

(1) Let the time step $h = 0.005$, and make driving system into chaotic state via iteration under given initial state $[x_1^{(0)}, x_2^{(0)}, x_3^{(0)}, x_4^{(0)}]$, then the driving system will produce four chaotic sequences, denoted by $[x_1, x_2, x_3, x_4]$.

(2) Four chaotic sub-sequences can be get via keeping $(M \times N)/4$ points in each chaotic sequences from $t = 5000\ h$. Join the four chaotic sub-sequences end to end to be a sequence $B_{1\times(M\times N)}$.

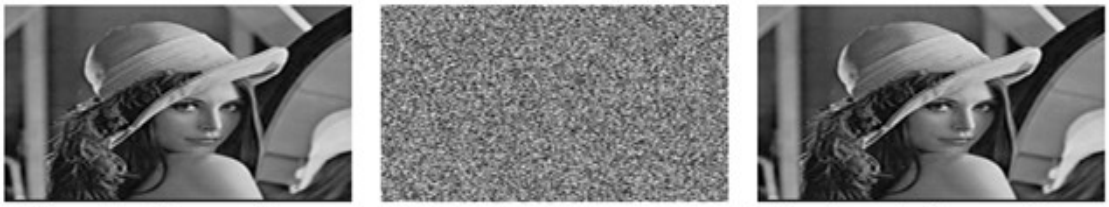
(3) In order to make operations between the sequence and image pixel matrix value, after amplifying sequence $B_{1\times(M\times N)}$, it is taken modular arithmetic with *A*, and $B'_{1\times(M\times N)}$ would be converted into the unsigned eight bit integer data for making the sequence value in the range from 0 to *A*, that is, $B'_{1\times(M\times N)}$ = mod (1000 * $B_{1\times(M\times N)}$, *A*), $B''_{1\times(M\times N)}$ = uint8 ($B'_{1\times(M\times N)}$);

(4) Carry out XOR operation between each element of $B''_{1\times(M\times N)}$ and g_{ij}, the value of g_{ij} is arranged in regular rows, then we get a new matrix $G' = (g'_{ij})_{M\times N}$ which denotes the image after being encrypted.

The process of decryption process is the inverse process of encryption process. At receiving terminal, use the secret key (the initial value of driving system) to make responsive system into chaotic state via iteration, and we can get four chaotic sequences. Then, according to the above step (2) - (4) of encrypting, assemble these sequences into a new sequence, finally, perform bitwise XOR between each element of the sequence and corresponding encrypted image G' in turn, then we can get the decrypted image.

5.1 The Simulated Results of Image Encryption and Decryption

In this section, we will apply tracking control synchronization in to encrypting Lena whose size is 256×256, and we will do simulation with matlab7.8. Let $x_1^{(0)} = 8, x_2^{(0)} = 4, x_3^{(0)} = 2, x_4^{(0)} = 1, \alpha = 0.95$, and the simulation results are shown in Figure 7.



(a)the original image of Lena (b)the encrypted image of Lena (c)the decrypted image of Lena

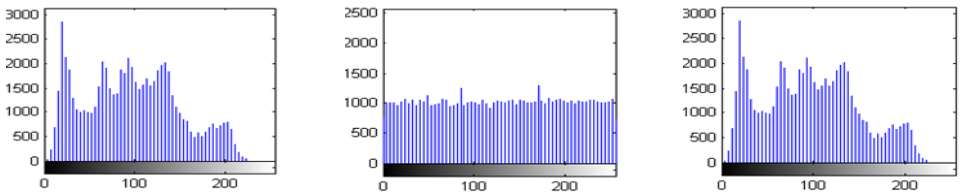
Fig 7 The simulation results of encryption and decryption

From Figure 7 (b), we can see that the encrypted images are very different from the original images. From Figure 7 (c), we can see that the encrypted images can be decrypted at the receiving terminal.

In order to furtherly check the validation of the method presented, Lena original image, its encrypted image and its decrypting image are compared in histogram and in correlation between adjacent pixels. We also analysis the sensitivity of the encrypted image to the secrete keys.

5.2 The Comparition of Histogram

The histograms of Lena original image, its encrypted image and its decrypted image are shown in Figure 8 (a), (b) and (c) respectively. It is clear that the histogram of the Lena original image is extremely similar to the one of the Lena decrypted image, but the histogram of Lena encrypted image is nearly even-distributed in the entire range of gray. It shows that statistical property of the original image has been broken, so the encrypted image has a good ability to resist the attack that is based on statistical characteristics.



(a) The histogram of original Lena image (b) The histogram of encryption image (c) The histogram decrypted image

Figure 8. The gray histogram

5.3 The Comparision of Correlation between Adjacent Pixels

Firstly, we randomly select 5×5 pixels from Figure 7(a) and (b) respectively, and the grey values of selected pixels are shown in table 1 and 2. It is clear that the grey values of pixels from the encrypted image have more change than the one from the original image. Furthermore, the difference of two gray values corresponding two adjacent pixels in the original image is small, but the one in the encrypted image is large.

Then we randomly select 1000 adjacent pixel pairs in horizontal, vertical and diagonal direction respectively from Figure 7(a) and (b), and the results are shown in table 3. It shows that all correlation coefficients in horizontal, vertical and diagonal directions are close to 1 in the original image, but they are close to 0 in the encrypted image. So the correlation of adjacent pixel in the original image has been broken via encrypting.

Tab.1 The grey values of the 5×5 pixels from the original image

138	133	134	134	136
133	133	133	130	134
129	133	130	130	133
131	133	130	122	132
131	130	130	130	132

Tab.2 The grey values of the 5×5 pixels from the encrypted image

67	222	154	215	5
224	61	146	100	254
175	102	52	253	17
12	22	176	191	86
13	67	172	158	205

Tab.3 The correlation coefficient of 1000 adjacent pixel-pairs in Lena image

Direction	The original Lena	The encrypted Lena
Horizontal	0.9723	-0.0141
Vertical	0.9437	-0.0217
Diagonal	0.9347	-0.0092

5.4 The Sensitivity of the Encrypted Image to the Secrete Keys

A chaotic system is very sensitive to initial state. If there are not completely correct secrete keys, the encrypted information can not be restored correctly. During the simulation experiment, if Figure 9(a) the encrypted Lena image is decrypted using the correct secrete key $x_1^{(0)} = 8$, $x_2^{(0)} = 4$, $x_3^{(0)} = 2$, we can get the right image shown in Figure 9(b); if it is decrypted using another secrete key $x_1^{(0)} = 8.0000000001$, $x_2^{(0)} = 4$, $x_3^{(0)} = 2$, $x_4^{(0)} = 1$, we can get another image shown in Figure 9(c). Because of a tiny difference 10^{-10} between the two keys, we can get two completely different results. This shows that the encrypted image is sensitive to secrete keys, and the encrypted image can be decrypted correctly only by the right keys.

(a)The encrypted Lena (b)The decrypted Lena under precision keys (c)The decrypted Lena under changed keys

Figure 9. Encrypt Lena image and its decrypted images

6. Conclusion

In this paper, we expanded a four-dimensional integral-order hyperchaotic system to be a fractional-order system, then we theoretically analyzed and quantitatively simulated some chaos characteristics.

We also put forward a method to synchronize two fractional-order chaos systems with different structures on the basis of the stability theory of fractional-order linear system and the tracking control ideas, and we gave the analysis formula of synchronous controller and carry out quantitative simulations on the synchronization between the extended fractional-order system and Rőssler hyperchaotic system.

At last we applied the proposed synchronization method to encrypting and decrypting digital images. Lena original image, its encrypted and decrypting image are compared in histogram and in correlation between adjacent pixels, we also analyzed the sensitivity of the encrypted image to the secrete keys. The experimental results show that this method has many advantages for encrypting and decrypting digital images.

7. The Future Work

At present, the synchronization method of integer-order system has been developed well, whether these approaches can be extended to fractional-order chaos or whether synchronization scheme will be put forward for fractional order system is worth considering. Another future work is reducing the amount of computation and improving the calculation accuracy of fractional calculus operations.

Acknowledgments

This work is partly supported by the grants from the National Science Foundation of China (NSFC) under Grant No.: 61063008 and Grant No.: 61163003, the Science Foundation of Yunnan Province of China under Grant No.: 2010CD025, the National Science Foundation of China (NSFC) under Grant No.: 6262069.

References

[1] Puyun Gao. *Nonlinear Dynamics. Changsha* : National Defense University Press. 2005.
[2] Hartly T T, Lorenzo C F, Qammer H K. Chaos in a fractional order Chua's system. *IEEE* Trans CAS-I. 1995; 42(8): 485-490.
[3] Arena P, Caponetto R, Fortuna L, Porto D. *Chaos in a fractional order duffing system*. In: Proceedings of ECCTD. Budapest. 1997: 1259–1262.
[4] Li C G, Chen G R. *Chaos and hyperchaos in the fractional-order Rössler equations*. Physica A. Volume 341: 55-61.
[5] Liu L, Liu C X, Zhang Y B. Analysis of a Novel Four-Dimensional Hyperchaotic System. *Chinese Journal of Physics*. 2008; 46(4): 386-393.
[6] Zhou Ping, Kuang Fei. *Synchronization between fractional-order chaotic system and chaotic system of integer orders.* Acta Physica Sinica. 2010; 59(10): 6851-6858.
[7] Rőssler, O.E. *An Equation for continuous chaos*. Physics Letters A. 1976; 57: 397-398.
[8] Rőssler, O.E. *An Equation for Hyperchaos*. Physics Letters A. 1979; 71(2-3): 155-157.
[9] Ivo Petráš. *Fractional-Order Nonlinear Systems: Modeling, Analysis and Simulation*. Beijing, China: Higher Education Press. 2011: 3.
[10] Deng,W. Short memory principle and a predictor-corrector approach for fractional differentional equations. *Journal of Computational and Applied Mathematics*. 2007; 206: 174-188.
[11] Matthews R. *On the Derivation of a Chaotic Encryption Algorithm*. Cryptologia. 1989; 13(1): 29-42.
[12] Christos K. Volos. Image Encryption Scheme Based on Coupled Chaotic Systems. *Journal of Applied Mathematics&Bioinformatics*. 2013; 3(1): 123-149.
[13] X. Wang, L. Teng and X. Qin. *A Novel Colour Image Encryption Algorithm Based on Chaos*. Signal Process, 2012; 92: 1101-1108.
[14] Z. Yunpeng, L.Wei, C. Shuiping, Z. Zhengjun, N. Xuan, D. Weidi. *Digital image encryption algorithm based on chaos and improved DES*. Systems, Man and Cybernetics, IEEE int. Coference. 2009: 474-479.
[15] G. Sansone and R. Conti. *Non-linear Differential Equations*. Pergamon Press. International Series of Monographs in Pure and Applied Mathematics. 1964; 67.
[16] Jianbing Hu. *Stability theory of fractional-order chaos and synchronization method*. China National Knowledge Infrastructure. 2008.
[17] A.Wolf, J.B.Swinney, H.L.Swinney, et al. *Determining Lyapunov exponents from a time series*. Physica D. 1985; 16: 285-317.
[18] Chen Guanrong, Mao Yaobin, Charles K. *A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps*. Chaos, Solitons and Fractals. 2004; 3(21): 749-761.